WHAT IS CLAIMED IS:

1   1. An apparatus for protecting a computer system,

2   comprising:

3   a password controller coupled to said computer system,

4   said password controller capable of receiving a password attempt

5   and capable of operating a computer program to compare said

6   password attempt with a stored password, wherein said stored

7   password comprises a password segment and said password segment

8   comprises:

9   an entry event comprising a predetermined entry

10   signal;

11   a predetermined time interval following said entry

12   event; and

13   a terminating signal following said predetermined

14   time interval, said terminating signal marking the end

15   of said password segment;

16   wherein said computer program is capable of allowing access to

17   said computer system when a password segment of said password

18   attempt matches said password segment of said stored password.

1   2.   The apparatus as set forth in Claim 1 wherein said

2   computer program is capable of comparing a time envelope of said

3   stored password with a time envelope of a received password

4   attempt, and capable of denying access to said computer system

5   when said time envelope of said received password attempt does

6   not match said time envelope of said stored password.

1   3.   The apparatus as set forth in Claim 1 wherein said

2   computer program compares said stored password with said

3   password attempt received from an online connection to determine

4   whether said password attempt from said online connection

5   matches said stored password.

1   4.   The apparatus as set forth in Claim 1 wherein said

2   entry event comprises a predetermined combination of computer

3   readable entry signals, wherein each computer readable entry

4   signal comprises one of: a character, a symbol, and a number.

1   5.   The apparatus as set forth in Claim 1 wherein said

2   terminating signal is an entry event that follows said

3   predetermined time interval.

1   6.   The apparatus as set forth in Claim 3 wherein said

2   computer program is capable of sending a signal to said online

3   connection that indicates whether said password attempt received

4   from said online connection matches said stored password.

1   7.   The apparatus as set forth in Claim 6 wherein computer

2   program is capable of waiting until a time delay period expires

3   before sending said signal that indicates whether said password

4   attempt received from said online connection matches said stored

5   password.

8.   The apparatus as set forth in Claim 7 wherein said time

delay period is of variable duration.

1   9.   The apparatus as set forth in Claim 1 wherein said

2   stored password comprises at least one password segment

3   comprising a predetermined time interval calculated by

4   subtracting from the total time measured from the trailing edge

5   of a first entry event to the trailing edge of a next second

6   entry event the time required to read said next second entry

7   event.

       10. The apparatus as set forth in Claim 2 wherein said

stored password further comprises a plurality of password

segments wherein the total time of said plurality of password

segments equals said time envelope of said stored password,

within a predetermined deviation.

1   11. An apparatus for protecting a computer system,

2   comprising:

3   a password controller coupled to said computer system,

4   said password controller capable of receiving a password attempt

5   and capable of operating a computer program to compare a time

6   envelope of a received password attempt with a time envelope of

7   a stored password, and capable of denying access to said

8   computer system when said time envelope of said received

9   password attempt does not match said time envelope of said

10   stored password.

36

1   12. A method of protecting an computer system, comprising

2   the steps of:

3   detecting an initial entry event of a password attempt;

4   determining whether a password segment of said password

5   attempt matches a password segment of a stored password wherein

6   said password segment comprises:

7   an entry event comprising a predetermined entry

8   signal;

9   a predetermined time interval following said entry

10   event; and

11   a terminating signal following said predetermined

12   time interval, said terminating signal marking the end

13   of said password segment; and

14   allowing access to said computer system when said

15   password segment of said password attempt matches said password

16   segment of said stored password.

1   13.   The method as set forth in Claim 12 further comprising

2   the step of:

3   calculating a time interval of said password segment

4   of said password attempt by subtracting the time required to

5   read a next second entry event from the total time measured from

6   the trailing edge of a first entry event to the trailing edge of

7   said next second entry event; and

8   determining whether said time interval of said password

9   segment of said password attempt matches a time interval of said

10 password segment of said stored password.

11   14.   The method as set forth in Claim 13 further comprising

12 the steps of:

13   waiting for a time delay period to expire after

14 determining whether said password attempt matches said stored

5   password; and

6   sending a signal that indicates whether said password

7   attempt matches said stored password.

1   15.   The method as set forth in Claim 14 wherein said time

2   delay period is of variable duration.

1   16.   The method as set forth in Claim 13 further comprising

2   the step of:

3   determining whether said entry event of each said

4   password   segment   of   said   password   attempt   matches   a

5   corresponding   entry   event   of   said   password   segment   of   said

6   stored password.

1   17.   The method as set forth in Claim 13 further comprising

2   the step of:

3   determining whether said time interval of said password

4   segment   of   said   password   attempt   matches   a   corresponding   time

5   interval of each said password segment of said stored password.

1   18.   The method as set forth in Claim 12 further comprising

2   the step of:

3   comparing each entry signal in said entry event in said

4   password segment of said password attempt with a corresponding

5   entry signal in said entry event of said password segment of

6   said stored password.

1   19.   The method as set forth in Claim 12 further comprising

2   the step of:

3   beginning the timing of said password segment of said

4   password attempt at the trailing edge of one of a first entry

5   event and first entry signal; and

6   concluding the timing of said password segment of said

7   password attempt at the trailing edge of one of a next second

8   entry event and next second entry signal.

1   20.   A method of protecting an computer system comprising

2   the steps of:

3   detecting an initial entry event of a password attempt;

4   comparing a password segment of said password attempt

5   to a password segment of a stored password;

6   determining whether said password attempt matches said

7   stored password;

8   waiting for a time delay period to expire after

9   determining whether said password attempt matches said stored

10   password; and

11   allowing access to said computer system when said

12   password attempt matches said stored password.

1   21.   The method as set forth in Claim 19 further comprising

2   the steps of:

3   comparing a time envelope of said stored password to

4   a time envelope of said password attempt;

5   determining whether a time interval of a password

6   segment of said password attempt matches a corresponding time

7   interval of said password segment of said stored password; and

8   calculating a time interval of said password segment

9   of said password attempt by subtracting the time required to

10 read a next second entry event from the total time measured from

11 the trailing edge of a first entry event to the trailing edge of

12 said next second entry event.

1   22. For use in a computer, computer executable process

2   steps stored on a computer readable storage medium capable of

3   protecting said computer, comprising the steps of:

4   detecting an initial entry event of a password attempt;

5   determining whether a password segment of said password

6   attempt matches a password segment of a stored password wherein

7   said password segment comprises:

8   an entry event comprising a predetermined entry

9   signal;

10   a predetermined time interval following said entry

11 event; and

12   a terminating signal following said predetermined

13 time interval, said terminating signal marking the end

14 of said password segment; and

15   allowing access to said computer system when said

16 segment of said password attempt matches said password segment

17 of said stored password.

1   23. The computer executable process steps stored on a

2   computer readable storage medium, as set forth in Claim 22,

3   further comprising the steps of:

4   calculating a time interval of said password segment

5   of said password attempt by subtracting the time required to

6   read a next second entry event from the total time measured from

7   the trailing edge of a first entry event to the trailing edge of

8   said next second entry event; and

9   determining whether said time interval of said password

10 segment of said password attempt matches a time interval of said

11 password segment of said stored password.

1   24. The computer executable process steps stored on a

2   computer readable storage medium, as set forth in Claim 22

3   further comprising the steps of:

4   waiting for a time delay period to expire after

5   determining whether said password attempt matches said stored

6   password; and

7   sending a signal that indicates whether said password

8   attempt matches said stored password.

1   25. The computer executable process steps stored on a

2   computer readable storage medium, as set forth in Claim 22,

3   further comprising the step of:

4   waiting an arbitrary and variable time delay period

5   before sending said signal that indicates whether said password

6   attempt signals matches said stored password.

1   26. The computer executable process steps stored on a

2   computer readable storage medium, as set forth in Claim 22

3   further comprising the step of:

4   determining whether said entry event of each said

5   password segment of said password attempt matches a

6   corresponding entry event of said password segment of said

7   stored password.

1   27. The computer executable process steps stored on a

2   computer readable storage medium, as set forth in Claim 22

3   further comprising the step of:

4   determining whether said time interval of said password

5   segment of said password attempt matches a corresponding time

6   interval of each said password segment of said stored password.

1   28.   The computer executable process steps stored on a

2   computer readable storage medium, as set forth in Claim 21

3   further comprising the step of:

4   comparing each entry signal in said entry event in said

5   password segment of said password attempt with a corresponding

6   entry signal in said entry event of said password segment of

7   said stored password.

29.   The computer executable process steps stored on a

computer readable storage medium, as set forth in Claim 22

further comprising the step of:

       beginning the timing of said password segment of said

password attempt at the trailing edge of one of a first entry

event and first entry signal; and

       concluding the timing of said password segment of said

8   password attempt at the trailing edge of one of a next second

9   entry event and next second entry signal.